



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/627,033

07/24/2003

John Gavan

COS94041C1

3709

25537

7590

12/08/2006

VERIZON

PATENT MANAGEMENT GROUP

1515 N. COURTHOUSE ROAD

SUITE 500

ARLINGTON, VA 22201-2909

EXAMINER

AGWUMEZIE, CHARLES C

ART UNIT

PAPER NUMBER

3621

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/627,033

Applicant(s)

GAVAN ET AL.

Examiner

Charlie C. Agwumezie

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 July 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-33 and 35-66 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-33, and 35-66 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>03/14/05; 07/24/03</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of Claims

1. Claims 4, and 34 are cancelled. Claims 1, 6, 7, 10, 13, 27-28, 30, 36, 54 and 66 are amended. Claims 1-3, 5-33, 35-66 are pending in this application per the response to office action filed on September 29, 2006.

Response to Arguments

2. Applicant's arguments with respect to claims 1-3, 5-33, and 35-66 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double

Art Unit: 3621

patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-3, 5-27, 28-33, and 35-66, are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 2, 5, 11, 14, 15, 18, 24, and 59 of U.S. Patent No. **7,117,191 B2**.

Although the conflicting claims are not identical, they are not patentably distinct from each other.

Claim 1 of the U.S. Patent No. 7,117,191 is obvious variant of claims 1, of the current application.

Claim 6 is obvious variant of Patent claims 2; Claim 10 is an obvious variant of Patent claim 5; Claim 28 is an obvious variant of Patent claim 11 and 14; Claim 5 is an obvious variant of Patent claim 15; Claim 59 is an obvious variant of Patent claim 18; Claim 24 is obvious variant of Patent claims 42 and 59.

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify claims 1, 2, 5, 11, 14, 15, 18, 24, and 59 of U.S. Patent No. **7,117,191 B2** by adding and/or substituting the limitations resulting generally in the claims of the present application since the present application and the claims recited in U.S. Patent No. 7,117,191 actually perform the same or similar function. It is well settled that the omission of an element and its function is an obvious

Art Unit: 3621

expedient if the remaining elements perform the same function as before. *In re Karlson*, 136 USPQ 184 (CCPA 1963; Also note *Ex parte Rainu*, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6, and 7-27, are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowman U.S. Patent Application No. 5,627,886 in view of Phelps U.S. Patent No. 5,602,906.

As per **claim 1**, Bowman discloses a method for detecting fraud in one of a credit card or debit card system, the system generating network event records, each network event record being generated in response to an event in the system, the method comprising the steps of:

(1) performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system (see fig. 2; col. 2, lines 15-25, 40-50; col. 3, line 60-col. 4, line 5; col. 17, lines 1-10...detecting

Art Unit: 3621

network usage pattern indicative of fraud...credit card usage and authorization records...);

(2) generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test (col. 2, lines 10-15, 25-40; col. 4, lines 25-35; col. 5, lines 35-45; ...alarm generation...).

What Bowman does not explicitly teach is

(3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and

(4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

Phelps discloses

(3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud (col. 2, lines 30-40; col. 2, line 63-col. 3, line 5; col. 4, lines 40-50); and

(4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case (col. 2, lines 30-40; col. 2, line 63-col. 3, line 5).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method of

(3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and (4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case in view of the teachings of Phelps in order to ensure that cases with high priority or severity level are given adequate attention and proper resolution.

As per **claims 2 and 32**, Bowman further discloses the method, wherein the method is performed by computer executable instructions disposed on at least one computer readable medium (fig 2).

As per **claims 3 and 33**, Bowman further discloses the method, wherein the computer executable instructions are distributed among a plurality of hardware platforms (fig. 2; col. 1, lines 45-60; col. 2, lines 25-40; ...detecting and monitoring disparate networks...).

As per **claim 5**, Bowman further discloses the method, wherein at least a portion of the computer executable instructions are implemented in a core infrastructure (fig. 1; network backbone connecting disparate networks as in fig. 1).

As per **claim 6**, Bowman discloses the method, wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event records conforms to a predetermined format (col. 7, lines 5-15).

As per **claims 7 and 37**, Bowman further discloses the method, wherein the at least one fraud detection test includes the step of enhancing the network event record such that an enhanced network event record includes data obtained from at least one external system (fig. 3; col. 6, lines 30-50; ...data incoming for fraud analysis...).

As per **claim 8**, Bowman further discloses the method, wherein the enhanced network event record includes data obtained from at least one database (fig. 2; col. 4, lines 50-60; ...RDBMS...primary database to store and maintain profile data etc...).

As per **claim 9**, Bowman further discloses the method, wherein the at least one database includes at least one of a configuration database, an event database, a billing database, a call history database, and/or a records database (fig. 2; col. 6, lines 5-30).

As per **claims 10 and 35**, Bowman further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event records to a threshold rule, the alarm being generated if one network event record violates the threshold rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claims 11 and 44**, Bowman further discloses the method, wherein the alarm is generated if a value in one network event record exceeds a threshold value specified by the threshold rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claim 12**, Bowman further discloses the method, wherein the alarm is generated if a value in the network event record does not equal a value specified by the threshold rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claim 13**, Bowman further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a profile detection rule, the alarm being generated if the network event record violates the profile detection rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claim 14**, Bowman further discloses the method, wherein the network event record is compared to a normal usage profile (col. 15, lines 40-65).

As per **claim 15**, Bowman further discloses the method, wherein the network event record is compared to a fraudulent usage profile (col. 15, lines 40-65).

As per claim 16, Bowman discloses the method, wherein the profile detection rule is based on historical network event records (col. 9, lines 10-35).

As per claim 17, Bowman further discloses the method, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a predetermined pattern to identify a normal usage and/or a fraudulent usage (col. 15, lines 40-65).

As per claim 18, Phelps further discloses the method, wherein the predetermined pattern is based on call history data (col. 9, lines 10-35).

missing motivation

As per claim 19, Bowman failed to explicitly disclose the method, wherein the predetermined pattern is generated by a neural network. Bowman however discloses that the system not only solves known fraud problems but also unknown fraud patterns.

Phelps further discloses the method, wherein the predetermined pattern is generated by a neural network (col. 1, lines 15-20).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate method, wherein the predetermined pattern is generated by a neural network in view of the teachings of Phelps in order to ensure that system solves unforeseen cases of fraud by

learning unknown patterns of fraud.

As per **claim 20**, Bowman further discloses the method, wherein the comparison is performed using tree-based algorithms that generate discrete output values (col. 7, lines 30-35).

As per **claim 21**, Bowman further discloses the method, wherein the comparison is performed using statistical based algorithms that that employ iterative numerical processing techniques (col. 7, lines 30-35).

As per **claim 22**, Bowman further discloses the method, wherein the step of correlating includes the step of enhancing a network event record by obtaining relevant data from an external source (fig. 3; col. 6, lines 30-50; ...data incoming for fraud analysis...).

As per **claim 23**, Bowman further discloses the method, wherein the step of correlating includes the step of applying at least one predetermined fraud analysis rule to the network event record to decide if a fraud case is appropriate (col. 13, lines 10-40).

As per **claim 24**, Bowman failed to explicitly disclose the method, wherein the step of correlating includes the step of applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case.

Phelps discloses the method, wherein the step of correlating includes the step of applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case (col. 1, lines 45-60).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the step of correlating includes the step of applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case in view of the teachings of Phelps in order to ensure that cases with high priority or severity level are given adequate attention and proper resolution.

As per claim 25, Bowman failed to explicitly disclose the method, wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority.

Phelps discloses the method, wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority (fig. 2; col. 5, lines 60-67).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority in view of the teachings of Phelps in order to ensure that cases with high priority or severity level are given adequate

Art Unit: 3621

attention and proper resolution.

As per **claims 26 and 65**, Bowman failed to explicitly disclose the method, wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification.

Phelps further discloses the method, wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification (col. 1, lines 45-60; col. 4, lines 1-10; col. 5, lines 5-20).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification in view of the teachings of Phelps in order to show the various method employed to archive resolution.

As per **claim 27 and 66**, Bowman failed to explicitly disclose the method, wherein the alarm is selected from a group that is comprised of at least one of a pin hacking alarm, or a geographic alarm. However, Bowman does teach that the system responds with an alarm when a threshold is met or exceeded.

Phelps also failed to explicitly designate its alarm as either pin hacking alarm or geographic alarm. Phelps teaches that an alert is generated when the threshold is exceeded. The threshold is dependent on the geographic dispersion of call origination point.

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the alarm is selected from a group that is comprised of at least one of a pin hacking alarm, or a geographic alarm in order to show the type of alarm designated or used.

As per claim 28, Bowman discloses a system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network, the system comprising:

a fraud detection system including a core computing infrastructure (backbone interconnecting disparate networks) and a domain specific infrastructure (object oriented), the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored, the core computing infrastructure (backbone connecting disparate networks) being non-domain specific, the fraud detection system being configured to analyze each network event record and perform a fraud prevention action in response to detecting an

Art Unit: 3621

occurrence of fraud in the network event record and based on whether the network is a credit card network or debit card network (fig. 2; col. 2, lines 40-67; col. 3, lines 5-40).

As per claim 29, Bowman further discloses the system, wherein the fraud detection system is dynamically reconfigured to adjust fraud detection rules in accordance with changing patterns of fraud (col. 3, lines 5-15; ...detects new types of fraud...).

As per claim 30, Bowman further discloses the system, wherein the fraud detection system further comprises:

a detection element coupled to the telecommunication system, the detection element being configured to generate a fraud alarm if the network event record is in violation of a predetermined fraud detection rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...);

an analysis element configured to receive fraud alarms from the detection element, the analysis element being configured to correlate fraud alarms having common aspects, and generate a fraud case based on correlated fraud alarms (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

What Bowman does not explicitly teach is

an expert element coupled to the analysis element, the expert element being configured to apply at least one predetermined expert rule to assign a priority

Art Unit: 3621

to the fraud case, the expert element performing a fraud prevention action in accordance with the priority.

Phelps discloses an expert element coupled to the analysis element, the expert element being configured to apply at least one predetermined expert rule to assign a priority to the fraud case, the expert element performing a fraud prevention action in accordance with the priority (col. 5, line 50-col. 6, line 25).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the system wherein an expert element coupled to the analysis element, the expert element being configured to apply at least one predetermined expert rule to assign a priority to the fraud case, the expert element performing a fraud prevention action in accordance with the priority in view of the teachings of Phelps in to ensure that cases with highest priority is treated according to its priority or severity level.

As per **claim 31**, Bowman failed to explicitly disclose the system, wherein the priority is based on a severity of suspected fraud.

Phelps further discloses the system, wherein the priority is based on a severity of suspected fraud (col. 4, lines 1-10).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the priority is based on a severity of suspected fraud in view of the teachings of Phelps in order to ensure that cases with high priority or severity level are given

Art Unit: 3621

adequate attention and proper resolution.

As per **claim 36**, Bowman further discloses the system, wherein the rules based thresholding engine further comprises:

at least one rules database (fig. 2; col. 6, lines 30-35);

a normalizer configured to configure the network event record in a standardized format (col. 7, lines 5-15; col. 8, lines 50-65; col. 9, lines 40-50);

an enhancer component coupled to the normalizer, the enhancer component being configured to insert additional data in the network event record (col. 16, lines 40-55); and

a threshold detector coupled to the enhancer component, the threshold detector being configured to compare a network event record to at least one threshold rule obtained from the at least one rules database, whereby the alarm is generated if the network event record violates the at least one threshold rule (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claim 38**, Bowman further discloses the system, wherein the network event record includes an event key and at least one feature, the event key identifying the network event and the at least one feature including event measurement data (col. 2, lines 25-40).

As per **claim 39**, Bowman further discloses the system, wherein the measurement data includes a count of a number of occurrences of an event during a predetermined time period (col. 15, lines 55-65; col. 16, lines 40-65).

As per **claim 40**, Bowman further discloses the system, wherein the measurement data includes a count of a number of like events occurring simultaneously (col. 16, lines 40-60).

As per **claim 41**, Bowman further discloses the system, wherein the measurement data includes geographic velocity data (col. 16, lines 60-65).

As per **claim 42**, Bowman further discloses the system, wherein the at least one database comprises:

an enhancement rules database coupled to the enhancer component, the enhancer component obtaining an enhancement rule from the enhancement rules database based on data in the network event record (fig. 2 and 3; col. 2, lines 40-64; "...including necessary billing information ..."); and

a threshold detection rules database coupled to the threshold detector, the threshold detector obtaining a threshold rule in accordance with data in the network event record (fig. 2; col. 2, lines 25-40).

As per **claim 43**, Bowman further discloses the system, wherein the enhancement rule directs the enhancer component to select external data from a selected external source (fig. 3; col. 6, lines 30-50; ...data incoming for fraud analysis...).

As per **claim 45**, Bowman further discloses the system, wherein the threshold rule stipulates that an alarm is generated when data in the network event record does not equal a threshold value (col. 2, lines 25-40; compares statistics ...to predefined thresholds and responds with an alarm...).

As per **claim 46**, Bowman further discloses the system, wherein the enhancer component provides the threshold detector with a feature vector, the feature vector including the event key and a plurality of feature event values, the event key including suspected fraud event identifying data, each feature event value of the plurality of feature event values providing fraud event measurement data (col. 2, lines 25-40).

As per **claim 47**, Bowman further discloses the system, wherein the feature event value includes a threshold value (col. 2, lines 25-40).

As per **claim 48**, Bowman further discloses the system, wherein the feature vector includes a name field, a value field, and a generating event field for each feature (col. 5, line 60-col. 5, line 5; ...event record is a collection of data fields...).

As per **claim 49**, Bowman further discloses the system, wherein the feature vector is implemented as a data structure, the data structure being stored on a computer readable medium (col. 3, lines 15-25).

As per **claim 50**, Bowman further discloses the system, wherein the feature vector includes at least one contributing event field for each feature (col. 5, line 60-col. 5, line 5).

As per **claim 51**, Bowman further discloses the system, wherein the at least one software processing engine in the detection element further comprises:

a profiling database including at least one profile detection rule (fig. 2; col. 4, lines 50-60); and

a profiling engine configured to compare the network event record with at least one profile in accordance with the at least one profile detection rule, the profiling engine generating the alarm if the network event record substantially violates the profile detection rule (fig. 2; col. 2, lines 25-40).

As per **claim 52**, Bowman further discloses the system, wherein the profile includes a normal use profile and/or a fraudulent use profile (col. 4, lines 50-60).

As per **claim 53**, Bowman further discloses the system, wherein the profile is based on historical network event records (col. 2, lines 10-15).

As per **claim 54**, Bowman further discloses the system, wherein the at least one software processing engine in the detection element comprises a pattern recognition engine configured to identify normal and/or fraudulent patterns of usage (col. 8, lines 50-65).

As per **claim 55**, Bowman further discloses the system, wherein the pattern recognition engine compares the network event record to call history data obtained from a call history database (col. 8, lines 50-65; col. 9, lines 10-35).

As per **claim 56**, Bowman further discloses the system, wherein the pattern recognition engine includes a neural network configured to identify fraudulent patterns of usage (col. 8, lines 50-65).

As per **claim 54**, Bowman further discloses the system, wherein the pattern recognition engine includes tree-based algorithms (col. 7, lines 30-35).

As per **claim 58**, Bowman further discloses the system, wherein the pattern recognition engine includes statistical based algorithms that that employ iterative numerical processing techniques (col. 7, lines 30-35).

As per **claim 59**, Bowman further discloses the system, wherein the analysis element further comprises:

an external systems interface component configured to obtain data from external systems relevant to the fraud alarms (fig. 2 and 3);

a configuration database configured to specify any additional data required for fraud alarm analysis (fig. 2);

an alarm enhancement component coupled to the external systems interface and the configuration database, the alarm enhancement component being configured to add the additional data and external system data to the fraud alarm (fig. 3; col. 6, lines 30-45); and

a fraud case builder component coupled to the alarm enhancement component, the fraud case builder being configured to correlate and consolidate fraud alarms (col. 10, line 10-25, 40-55).

As per **claim 60**, Bowman further discloses the system, wherein the fraud case builder is coupled to a rules database, the rules database providing the fraud case builder with parameters for generating fraud cases (col. 10, line 10-25, 40-50).

As per **claim 61**, Bowman further discloses the system, wherein the expert element further comprises:

Art Unit: 3621

a configuration database configured to specify any additional data required for alarm analysis based on an alarm configuration (fig. 2);

an external systems interface component configured to obtain data from external systems relevant to at least one of the alarms (fig. 3);

a prioritizer component coupled to the configuration database and the external systems interface, the prioritizer being configured to direct the external system interface to obtain the additional data from at least one external system based on configuration data obtained from the configuration database, the prioritizer adding the additional data to the fraud case (fig. 3; col. 6, lines 20-30...obtains additional data at least from billings and according to customer selected criteria...).

What Bowman does not explicitly disclose is prioritizer.

Phelps discloses a prioritizer (col. 4, lines 1010)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein there is a prioritizer component in view of the teachings of Phelps in order to ensure that cases are prioritized according to severity level so that adequate attention and proper resolution is given to such cases.

As per claim 62, Bowman failed to explicitly disclose the system, wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud cases in accordance with the prioritization rules.

Phelps further discloses the system, wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud cases in accordance with the prioritization rules (col. 4, lines 1010).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud cases in accordance with the prioritization in view of the teachings of Phelps in order to ensure that cases are prioritized according to severity level so that adequate attention and proper resolution is given to such cases.

As per claim 63, Bowman failed to explicitly disclose the system, wherein the prioritization rules specify the fraud prevention action.

Phelps further discloses the system, wherein the prioritization rules specify the fraud prevention action (col. 5, lines 5-20; col. 6, lines 1-25).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method wherein the prioritization rules specify the fraud prevention action in view of the teachings of Phelps in order to ensure that cases are prioritized according to severity level so that adequate attention and proper resolution is given to such cases.

As per claim 64, Bowman failed to explicitly disclose the system, further comprising an enforcement component coupled to the prioritizer component, the

Art Unit: 3621

enforcement component performing the fraud prevention action based on the enhanced fraud case.

Phelps further discloses the system, further comprising an enforcement component coupled to the prioritizer component, the enforcement component performing the fraud prevention action based on the enhanced fraud case (col. 5, lines 5-20; col. 6, lines 1-25).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the system, further comprising an enforcement component coupled to the prioritizer component, the enforcement component performing the fraud prevention action based on the enhanced fraud case in view of the teachings of Phelps in order to ensure that cases are prioritized so that adequate attention and proper resolution is given to such cases.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of

Art Unit: 3621

the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

**Commissioner of Patents and Trademarks
Washington D.C. 20231**

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Art Unit: 3621

Hand delivered responses should be brought to the United States Patent and
Trademark Office Customer Service Window:

Randolph Building,

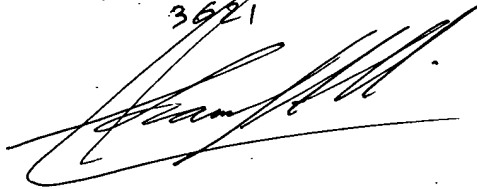
401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
December 5, 2006

KAMBIZ ABDI
PRIMARY EXAMINER

3621

A handwritten signature in black ink, appearing to read 'Kambiz Abdi', is written over the printed name and title. The signature is stylized with a large, sweeping initial 'K'.